Deutscher Bundestag **Drucksache 17/7760**

17. Wahlperiode 17. 11. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Korte, Andrej Hunko, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/7104 –

Auskunft über Einsatz staatlicher Schadprogramme zur Computerspionage („Staatstrojaner“)

Vorbemerkung der Fragesteller

Am 8. Oktober 2011 veröffentlichte der Hamburger Chaos Computer Club e. V. (CCC) eine 20-seitige Analyse eines ihm in mehrfacher Ausführung zugespielten Schadprogrammes zur Computerspionage (www.ccc.de/de/updates/2011/staatstrojaner). Der CCC kommt zu dem Schluss, dass es sich bei den ihm zugesendeten Trojanern um eine staatliche Software handele, mit der Ermittlungsbehörden die Computer von Verdächtigen ausspähen können.

Die Analyse der extrahierten Binärdateien der Software mache deutlich, dass die Trojaner unter anderem in der Lage seien, weitere Software über das Internet nachzuladen, darunter auch Programme, die eine gegebenenfalls am Zielrechner installierte Webcam zur Raumüberwachung nutzen könnten. Außerdem könnten die Trojaner Programmteile verändern, nicht gesendete E-Mails kopieren und vor allem Dateien auf dem Rechner unbemerkt und ohne Spuren zu hinterlassen, hinterlegen. Damit wären die technischen Möglichkeiten des Programms, also umfängliche Manipulationen an dem Zielrechner vorzunehmen, für staatliche Stellen verfassungswidrig, da die Funktionalität der Software weit über die Grenzen dessen hinaus geht, was das Bundesverfassungsgericht (BVerfG) in seinem Urteil im Jahre 2008 (www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html) vorgegeben hat. Hinzu kommt, dass der Trojaner aufgrund seiner „schlampigen Programmierung“ laut CCC weitere massive Sicherheitslücken enthält. Problematisch bei der Software, sei nach Angaben des CCC der Umstand, dass die ausgespähten Daten zur Verschleierung der Steuerzentrale für die Überwachung über einen „command-and-control“-Server (C+C) in den USA umgeleitet wurden. So könnten Daten ohne großen Aufwand von amerikanischen Dienststellen mitgelesen werden, denn alle US-IT-Firmen sind zur Kooperation mit diesen und entsprechenden Herausgabe der Daten gesetzlich verpflichtet.

Das Bundesministerium des Innern (BMI) widersprach am 9. Oktober 2011 Aussagen, dass es sich bei der Schadsoftware um „Bundes-Trojaner“ handele, die auch von Behörden der Bundesregierung eingesetzt worden seien: „Das Bundeskriminalamt hat den sogenannten Trojaner nicht eingesetzt.“ Und wei-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 15. November 2011 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

ter: „Im Übrigen sind die zuständigen Justiz- und Sicherheitsbehörden des Bundes und der Länder jeweils eigenständig für die Einhaltung technischer und rechtlicher Vorgaben verantwortlich.“ Die Bundesministerin der Justiz, Sabine Leutheusser-Schnarrenberger, hat angesichts der Vorwürfe des angeblichen Bundestrojaners „totale Transparenz und Aufklärung“ versprochen. Sie werde auf Bundes- und Länderebene prüfen, ob solch eine Überwachung in Deutschland zum Einsatz komme. Im ARD-„Morgenmagazin“ erklärte die FDP-Politikerin am 10. Oktober 2011: „Wenn das so wäre, wäre es nicht im Einklang mit unseren Gesetzen“, dann müssten geeignete Wege gefunden werden, das zu untersagen. Der Vorsitzende des Innenausschusses des Deutschen Bundestages, Wolfgang Bosbach (CDU), gab gegenüber den Medien zu, dass einigen Mitgliedern des Innenausschusses einmal eine Software vorgeführt worden sei, die die vom CCC beschriebenen Fähigkeiten aufweise. „Man sei sich deswegen im Ausschuss schnell einig gewesen, dass diese Software nicht angeschafft werde“ (vgl. Süddeutsche Zeitung vom 10. Oktober 2011). Aus dem Zeitungsbericht war allerdings nicht ersichtlich, ob der exklusive Kreis einzelner Mitglieder des Innenausschusses daraufhin den Hersteller der Software auf die Illegalität eines Einsatzes der beworbenen Software in der Bundesrepublik Deutschland hingewiesen hatte.

Mittlerweile haben sich Vermutungen bestätigt, dass mindestens einer der Trojaner aus Bayern stammt (vgl. heise online vom 10. Oktober 2011) und dort bereits mehrfach in Ermittlungsverfahren eingesetzt wurde. Am 10. Oktober 2011 gab der Minister des Bayerischen Staatsministeriums des Innern Joachim Herrmann bekannt, die vom CCC analysierte Software stehe in Zusammenhang mit einem Ermittlungsverfahren im Jahr 2009. Die 4. Strafkammer des Landgerichts Landshut hat in ihrem Beschluss vom 25. Januar 2011 den Einsatz dieses „Bayerntrojaners“ für rechtswidrig erklärt.

Programmiert wurde die Software von der privaten hessischen Firma DigiTask (www.digitask.de/).

Laut Angaben der jeweiligen Innenminister wurden Trojaner von den Ermittlungsbehörden der Länder Niedersachsen, Rheinland-Pfalz, Bayern, Brandenburg und Bremen eingesetzt. Während die Innenministerien von Sachsen und Hessen zunächst nicht auf Anfragen des „SPIEGEL“ reagierten, kündigte das Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen an, Erkundigungen einzuleiten, um herauszufinden ob Trojaner in Nordrhein-Westfalen bereits zum Einsatz kamen (vgl. DER SPIEGEL vom 10. Oktober 2011). Das Bundeskriminalamt (BKA) prüft unterdessen, ob weitere Landesbehörden Trojaner eingesetzt haben (vgl. Reuters vom 10. Oktober 2011). Am 10. Oktober 2011 stoppte Baden-Württemberg den Einsatz der Software. Der Innenminister des Landes Baden-Württemberg Reinhold Gall (SPD) räumte ein, bis zu diesem Zeitpunkt sei von der baden-württembergischen Polizei dieselbe Basisversion des Trojaners wie in Bayern verwendet worden.

Behauptet wird, bei anderen Behörden sei andere Schnüffelsoftware im Einsatz als der vom CCC untersuchte Staatstrojaner, den die Firma DigiTask nach eigenen Angaben im November 2008 an das Bayerische Landeskriminalamt lieferte. Der Geheimdienstkoordinator im Bundeskanzleramt wird inzwischen aber damit zitiert, dass die Landesbehörden multifunktionale Rohlinge erhalten hätten, die als Prototypen weit mehr Fähigkeiten als rechtlich zugelassen besäßen und die dann von den Ermittlern auf die jeweils vom Gericht zugelassenen Funktionen reduziert werden sollten (vgl. dpa-Meldung vom 13. Oktober 2011). Die Firma DigiTask, die entsprechende Software zur Telekommunikationsüberwachung in die Niederlande, nach Österreich, in die Schweiz und in Deutschland an „Ermittlungsbehörden auf Landes- und Bundesebene“ verkauft, dürfte mit öffentlichen Aufträgen in den vergangenen Jahren Millionen von Euro umgesetzt haben (vgl. SPIEGEL ONLINE vom 11. Oktober 2011). Nach Angaben des „SPIEGEL“ verlautete aus „Berliner Sicherheitskreisen“, dass das Bundeskriminalamt ebenfalls Software der Firma DigiTask einsetzt – allerdings angeblich nur in modifizierter Version. „Experten hätten die auch von Bayern eingesetzte Version begutachtet und für zu weitgehend befunden. DigiTask habe seine Software nach den Vorgaben von BKA und Bundesinnenministerium angepasst.“ (SPIEGEL ONLINE von 12. Oktober 2011).

Das Bundesministerium der Finanzen teilte unterdessen mit, dass die Zollbehörden in bislang 16 Fällen Spionageprogramme eingesetzt hätten, deren Einsatz aber sei „in einem engen rechtlichen Rahmen und nur zur Überwachung von verschlüsselten Telefonaten“ erfolgt (Frankfurter Allgemeine Zeitung vom 13. Oktober 2011). Im Amtsblatt der Europäischen Union gab das Zollkriminalamt für die Jahre 2008 und 2009 mehrere Aufträge zur Lieferung von Hard- und Software zur Telekommunikationsüberwachung bekannt: 2008 seien demnach für insgesamt 760 000 Euro zwei Aufträge über „TKÜ Auswerte -SW“ und „TKÜ Auswerte Hardware u. Softwarelizenzen“ an die Firma DigiTask vergeben worden (Amtsblatt der Europäischen Union vom 14. März 2008). 2009 folgte ein weiterer Auftrag über 2,1 Mio. Euro ebenfalls an die Firma DigiTask für die „Lieferung von Hard- und Software zur Telekommunikationsüberwachung (TKÜ)“ (Amtsblatt der Europäischen Union vom 29. Januar 2009). Die Firma DigiTask erhielt ferner den Zuschlag durch das Zollkriminalamt für den Auftrag zur „Hardware-Instandhaltungs- und Software-Pflegeleistungen an stationären Telekommunikationsüberwachungsanlagen“ über 700 000 Euro (Amtsblatt der Europäischen Union vom 23. Januar 2009).

Am 19. Oktober 2011 berichtete der „SPIEGEL“, dass der Anti-Viren-Software-Hersteller Kaspersky nach eigenen Angaben eine weitere Version des Staatstrojaners analysiert und dabei festgestellt habe, das das offenbar ebenfalls von der Firma DigiTask entwickelte Programm weitaus mehr Programme abhören kann, als der vom CCC identifizierte Bayern-Trojaner. Auch neuere Betriebssysteme soll der Schädling infizieren können (SPIEGEL ONLINE von 19. Oktober 2011).

Nachdem die Bundesregierung am 21. Mai 2010 in ihrer Antwort auf eine entsprechende Kleine Anfrage der Fraktion DIE LINKE. (Bundestagsdrucksache 17/1814) angab, dass bis Mai 2010 keine einzige Onlinedurchsuchung durch das Bundeskriminalamt vorgenommen worden sei, verweigerte die Bundesregierung in ihrer Antwort am 7. Juni 2011 auf die Kleine Anfrage „Anwendung von Onlinedurchsuchungen“ (Bundestagsdrucksache 17/6079) jegliche Information über die Anzahl durchgeführter Onlinedurchsuchungen, da dies eine „Offenlegung sensibler polizeilicher Vorgehensweisen und Taktiken” der Gefahrenermittlungen des BKA oder des Bundesnachrichtendienstes (BND) darstellen würde.

Inzwischen wurde offenkundig, dass mit ERA IT SOLUTIONS AG auch eine schweizer Firma in den Skandal um die ausufernde Nutzung staatlicher Trojaner-Programme involviert ist. Der Minister für Inneres und Kommunales des Landes Nordrhein-Westfalen hatte etwa zugegeben, dass das Land auch Software des schweizer Unternehmens für Quellen-TKÜ nutzt (Presseinformation vom 13. Oktober 2011). Die Software der Firma DigiTask wurde indes laut einem Bericht der „Neuen Zürcher Zeitung“ vom 15. Oktober 2011 genutzt, um schweizer Computer zu infiltrieren: Demnach stellte die schweizerische Bundeskriminalpolizei ein Rechtshilfegesuch an deutsche Behörden, damit diese den Mail-Verkehr und die Telefongespräche einer Züricher Linksaktivistin abhören. Hierfür wurde von der Firma DigiTask angeblich ein „Mietgerät mit Spezialsoftware“ für 26 000 Euro überlassen. Das Attackieren ausländischer Rechner mit deutschen Trojanern war bislang nur vom Auslandsgeheimdienst BND bekannt, der gemäß dem Nachrichtenmagazin „FOCUS“ vom 29. März 2009 in 90 Fällen Computer in Afghanistan und im Kongo infiltrierte. Grenzüberschreitende Einsätze von staatlichen Trojanern stellen einen Eingriff in die Hoheitsrechte anderer Regierungen dar.

Mit der Überprüfung der vom CCC aufgedeckten Verwendung mindestens eines Trojaners, der verfassungswidrige Eingriffe in den privaten Kernbereich von überwachten Personen ermöglicht und bei dem es sich technisch um eine Onlinedurchsuchung handelt, will die Bundesregierung nach offiziellen Verlautbarungen anscheinend offener umgehen. Die Bundeskanzlerin Dr. Angela Merkel erklärte, sie würde sich zu den laufenden Ermittlungen auf dem Laufenden halten lassen, auch das BKA werde die Verwendung von Schadprogrammen in den Ländern überprüfen (Reuters, 10. Oktober 2011). Das BKA bestätigte zudem, es habe schon bei der Programmierung der Software zwischen BKA und Landeskriminalämtern einen „Austausch auf Expertenebene“ gegeben (zeit.de

vom 12. Oktober 2011). Und nicht zuletzt hat die Bundesministerin Sabine Leutheusser-Schnarrenberger Transparenz im Umgang bei der Aufarbeitung des Skandals zugesagt. Wenn diese Zusagen eingehalten wurden, kann also davon ausgegangen werden, dass die Bundesregierung mittlerweile über ausreichendes Wissen über die Vorgänge in den Ländern und in den eigenen Behörden besitzt, um die folgenden Fragen zu beantworten.

Vorbemerkung der Bundesregierung

Die durch den Chaos Computer Club (CCC) analysierte und als „Bundestrojaner" bezeichnete Software ist nicht von Behörden des Bundes eingesetzt worden. Nach Pressemeldungen wurde die Software dem CCC zugänglich gemacht, indem der Rechtsanwalt eines von einer Quellen-TKÜ Betroffenen den PC bzw. die Festplatte seines Mandanten mit der aufgespielten Software an den CCC weitergegeben haben soll. Dabei handelte es sich nicht um ein durch das Bundeskriminalamt durchgeführtes Ermittlungsverfahren.

I. Fragen zum vom CCC analysierten Staatstrojaner

1. In wie vielen Fällen wurde die vom CCC analysierte Überwachungssoftware durch Sicherheitsbehörden des Bundes und der Länder bislang eingesetzt (bitte einzeln aufschlüsseln nach jeweiliger Behörde, Anlass für den Einsatz, konkretem Straftatverdacht, Rechtsgrundlage der Maßnahme, Anzahl der betroffenen Personen, Zeitpunkt und Dauer der Überwachungsmaßnahme, konkrete Einsatzfunktion – Kommunikationsüberwachung, Ausspähung und/oder Kopieren privater Daten (Speicherzugriff), Nachladen von Programmen, Kontrolle über den Rechner, Raumüberwachung usw.)?

Die vom CCC analysierte Software wurde von Bundesbehörden nicht eingesetzt. Die Bundesregierung verfügt nicht über eigene Erkenntnisse darüber, ob Behörden der Länder diese Software eingesetzt haben.

2. Bei welchen Bundesbehörden wird Trojaner-Software eingesetzt, die im Wesentlichen dem Quellcode des vom CCC analysierten Schadprogramms entspricht bzw. auf einem ähnlichen Installer basiert?

Der Quellcode der analysierten Software liegt der Bundesregierung nicht vor. Daher ist eine Aussage dazu nicht möglich.

Überwachungssoftware zur Durchführung von Quellen-TKÜ wurde bislang vom Bundeskriminalamt (BKA), dem Bundesamt für Verfassungsschutz (BfV) und dem Zollfahndungsdienst eingesetzt.

3. Wer gab wann wem den Auftrag zur Entwicklung der vom CCC analysierten Schadsoftware?

Auf die Antwort zu Frage 1 wird verwiesen. Der Bundesregierung liegen keine über Presseverlautbarungen hinausgehenden Informationen vor.

4. Wann wurde die Schadsoftware von wem angeschafft, wie hoch waren die Kosten dafür, und wie viele Versionen existierten bzw. existieren davon?

5. Wer gab die Entwicklung weiterer softwarespezifischer Funktionen, z. B. Nachladen weiterer Programme, Zugriff auf Festplatten und den darauf gespeicherten Datenbestand, Kontrolle über den Rechner, Möglichkeiten zur

Nutzung der Hardware zur akustischen Raumüberwachung usw., aus welchen Gründen, und auf welcher Rechtsgrundlage in Auftrag?

Auf die Antworten zu den Fragen 1 und 3 wird verwiesen.

6. Inwiefern wurde Überwachungssoftware, die von Bundesbehörden genutzt wird, in jedem Einzelfall auf die Einhaltung der Vorgaben aus der Entscheidung des Bundesverfassungsgerichtes zur sogenannten Onlinedurchsuchung geprüft, und wenn ja, mit welchem Ergebnis?

   Aus welchem Grund wurde eine derartige verfassungsrechtliche Prüfung in welchen Fällen unterlassen?

Die von Bundesbehörden eingesetzte Software wurde in jedem Einzelfall durch Anwendungstests auf die Einhaltung der einschlägigen Vorgaben geprüft. Ergebnis der Prüfung war jeweils, dass die Vorgaben eingehalten wurden. Auf die Antwort zu Frage 9 wird verwiesen.

7. Wie wurde die Qualitätssicherung bei der Herstellung, Anwendung sowie Auswertung der jeweils von Bundesbehörden eingesetzten Schadprogramme sichergestellt?

Die Qualitätssicherung bei der Herstellung der Software oblag dem Unternehmen, das sie entwickelt hat. Die Sicherung des Funktionsumfangs bei der Anwendung der Software erfolgte im Rahmen der in der Antwort auf Frage 6 beschriebenen Testmaßnahmen.

Darüber hinaus werden alle Daten, die an die Überwachungssoftware gesendet oder von dieser empfangen werden, protokolliert.

8. Warum wurde bei einem ggf. vorliegenden Verstoß gegen verfassungsrechtliche Vorgaben die Software dennoch erstellt bzw. angeschafft?

Auf die Antwort zu Frage 6 wird verwiesen.

9. Hatten die beauftragenden Behörden den Quellcode der jeweils eingesetzten Software vorliegen?

   Wenn nein, warum nicht?

Nein. Der Quellcode einer vermarkteten Software wird als Vermögenswert eines Unternehmens beurteilt und demzufolge als Geschäfts- und Betriebsgeheimnis geschützt. Die Bereitstellung eines Quellcodes ist im Bereich der Privatwirtschaft daher unüblich. Den beauftragenden Bundesbehörden lag der Quellcode nicht vor. Anstelle einer Quellcodeanalyse führten Bundesbehörden in jedem Einzelfall Anwendungstests durch.

10. War nach Kenntnis der Bundesregierung den beauftragenden Behörden vor dem ersten Einsatz der Software bekannt, dass der Zugriff auf die Software ohne Authentifizierung stattfindet und auch von nicht autorisierten Personen weitere Software implementiert und zur Ausführung gebracht werden kann, oder wurde die Software mit dieser Funktionalität ohne Auftrag und Wissen der Auftraggeber der Firma DigiTask ausgestattet?

Auf die Antworten zu den Fragen 1 und 3 wird verwiesen. Im Übrigen verwendet die vom CCC analysierte Software eine elektronische Markierung der

Kommunikationsdaten (Banner-String) zur Authentisierung. Der Zugriff nicht autorisierter Personen auf die Überwachungssoftware ist allenfalls eine theoretische Möglichkeit, da der potentielle Missbraucher über IP-Adresse, Übertragungsprotokoll, Kenntnis des Verschlüsselungsverfahrens und Schlüssel verfügen müsste. Die Bundesregierung hat keine Hinweise darauf, dass diese Informationen vor Veröffentlichung der Analyseerkenntnisse des CCC vorlagen.

11. Wie ist die Gewährleistung für die Software vertraglich geregelt, und erwägt die Bundesregierung Regressansprüche gegen die Herstellerfirma, für den Fall, dass sich herausstellen sollte, das diese die Verantwortung für den grundgesetzwidrigen Leistungsumfang ihres Produkts trägt (bitte begründen)?

Die Beschaffung der durch Bundesbehörden eingesetzten Überwachungssoftware wurde mit standardisierten Verträgen über die zeitlich befristete Überlassung von Standardsoftware (EVB-IT Überlassung Typ B) durchgeführt. Bestandteil der Verträge sind die Ergänzenden Vertragsbedingungen (EVB-IT Überlassung Typ B – Vertragsbedingungen), in denen unter anderem auch Bestimmungen zur Gewährleistung aufgeführt sind.

Die an Bundesbehörden gelieferte Software erfüllte alle Kriterien der dem einzelnen Beschaffungsvorhaben zugrundeliegenden Leistungsbeschreibung. Im Übrigen wird auf die Antworten zu den Fragen 1 und 3 verwiesen.

12. Sind nach Kenntnis der Bundesregierung weitere Versionen der Software in Entwicklung, und wenn ja, welche Eigenschaften sollen diese Software-Versionen bekommen?

Der Bundesregierung ist lediglich die Stellungnahme der Fa. DigiTask gegenüber ihren Kunden bekannt. Darin führt das Unternehmen aus, dass ein Prototyp zur Weiterentwicklung der Überwachungssoftware existiert, der unter anderem verbesserte Sicherheitsvorkehrungen (z. B. maßnahmenspezifische Verschlüsselung) aufweist.

13. Ist der Einsatz der vom CCC analysierten Software aus Sicht der Bundesregierung angemessen und gerechtfertigt, und wenn ja, in welchen Fällen und auf welcher Rechtsgrundlage?

    Wenn nein, warum nicht und welche Konsequenzen zieht sie daraus?

Die vom CCC analysierte Software wurde von Bundesbehörden nicht eingesetzt. Aufgrund der Veröffentlichung des CCC ist die Verwendung der analysierten Software nicht mehr möglich. Im Übrigen liegen der Bundesregierung keine über die Pressemeldungen hinausgehenden Erkenntnisse vor, wann und in welchem Verfahren die vom CCC analysierte Software eingesetzt wurde.

II. Fragen zum Einsatz von Staatstrojanern allgemein und zur technischen Kontrolle der Schadsoftware

14. Welche Bundesbehörden haben zu welchem genauen Zeitpunkt die Entwicklung, den Kauf oder die Lizenzierung von welcher Softwarelösung mit welchem Leistungsumfang und welcher Funktionalität zur Telekommunikationsüberwachung bei welcher Firma und zu welchen Kosten in Auftrag gegeben?

    Trifft es zu, dass eine „Onlineaktualisierung“, also Code-Nachladen, Bestandteil des Angebots bzw. des Pflichtenheftes war?

Die Überwachungssoftware wird in jedem Einzelfall gemäß der richterlichen Anordnung bzw. des Beschlusses der G 10-Kommission erstellt. Die damit verbundenen Kosten lassen sich wie folgt darstellen; soweit keine andere Angabe erfolgt, ist Vertragspartner die Fa. DigiTask:

Zahlungsdatum	Leistung	Kosten
Bundeskriminalamt		
2007	Überwachungssoftware	17 785 Euro
29. August 2008	Testgestellung	5 950 Euro
21. September 2009	Überwachungssoftware	4 165 Euro
7. Dezember 2009	Überwachungssoftware	4 165 Euro
1. März 2010	Überwachungssoftware	4 165 Euro
30. September 2010	Überwachungssoftware	4 760 Euro
11. Oktober 2010	Überwachungssoftware	12 495 Euro
7. Dezember 2010	Überwachungssoftware	17 255 Euro
26. Januar 2011	Überwachungssoftware	15 470 Euro
17. Februar 2011	Überwachungssoftware	7 735 Euro
22. März 2011	Testgestellung Gamma Group/Elamann	500 Euro
4. Mai 2011	Jährliche Generallizenz	199 920 Euro

Zahlungsdatum	Leistung	Kosten
Zollfahndungsdienst		
2007	Überwachungssoftware der Fa. ERA-Solution	11 700 Euro
2007	Überwachungssoftware der Fa. ERA-Solution	8 225 Euro
2007	Überwachungssoftware der Fa. ERA-Solution	10 700 Euro
2009	Überwachungssoftware	15 470 Euro
2009	Überwachungssoftware	2 975 Euro
2009	Überwachungssoftware	2 975 Euro
2009	Überwachungssoftware	34 263 Euro
2010	Überwachungssoftware	17 255 Euro
2010	Überwachungssoftware	29 750 Euro
2010	Überwachungssoftware	16 065 Euro

Darüber hinaus wurde für das BKA und den Zollfahndungsdienst in weiteren Verfahren Überwachungssoftware angeschafft, für die noch keine Rechnung erstellt worden ist bzw. aus anderen Gründen keine Kosten angefallen sind.

Der Bundesnachrichtendienst (BND) erhebt gemäß § 1 Absatz 2 Satz 1 des Bundesnachrichtendienstgesetzes (BNDG) Informationen von außen- und sicher-

heitspolitischer Bedeutung über das Ausland auch durch informationstechnische Operation.

Eine schriftliche Antwort der Bundesregierung auf diese und eine Reihe der folgenden Fragen würde spezifische Informationen zur Tätigkeit, insbesondere zur nachrichtendienstlichen Methodik des BND einem nicht eingrenzbaren Personenkreis – auch der Bundesrepublik Deutschland möglicherweise gegnerisch gesinnten Kräften – nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei könnte die Gefahr entstehen, dass seine operativen Fähigkeiten und Methoden aufgeklärt würden. Nicht zuletzt zum Schutz der Arbeitsfähigkeit und der Aufgabenerfüllung des BND – und damit zum Schutz der Sicherheit der Bundesrepublik Deutschland – muss dies verhindert werden.

Daher muss bei der Beantwortung dieser Anfrage eine Abwägung der verfassungsrechtlich garantierten Informationsrechte des Deutschen Bundestages und seiner Abgeordneten einerseits mit den dargestellten negativen Folgen für die künftige Arbeitsfähigkeit und Aufgabenerfüllung des BND sowie der daraus resultierenden Beeinträchtigung der Sicherheit der Bundesrepublik Deutschland und der Gefährdung für die Mitarbeiter des BND andererseits erfolgen. Bezogen auf die vorliegende Frage führt die gebotene Abwägung zum Vorrang der Geheimhaltungsinteressen. Zur Wahrung der Informationsrechte der Abgeordneten wird auf die Hinterlegung einer ergänzenden, VS-GEHEIM-eingestuften Antwort in der Geheimschutzstelle des Deutschen Bundestages verwiesen.*

Soweit sich die Frage auf die gemäß § 1 Absatz 1, § 3 Absatz 1 und 2 G10-Gesetz durchgeführte Quellen-TKÜ des Bundesamtes für Verfassungsschutz (BfV) bezieht, kann eine detaillierte Antwort an dieser Stelle ebenfalls nicht erfolgen.

Durch die detaillierte Kenntnis über die Durchführung derartiger Maßnahmen durch das BfV würde die Möglichkeit gegeben, aus der genannten Anzahl Rückschlüsse auf die Nutzungsintensität des vorgenannten nachrichtendienstlichen Mittels und damit mittelbar auf die Arbeitsweise des BfV zu gewinnen. Dass dies nicht geschieht, muss zum Schutz der Arbeitsfähigkeit und der Aufgabenerfüllung des BfV – und damit mittelbar zum Schutz der Sicherheit der Bundesrepublik Deutschland – sichergestellt bleiben.

Nach sorgfältiger Abwägung ist die Bundesregierung daher zu der Auffassung gekommen, dass die detaillierte Auskunft über die Quellen-TKÜ des BfV geheimhaltungsbedürftig ist. Die Bundesregierung wird das Informationsrecht des Deutschen Bundestages unter Wahrung berechtigter Geheimhaltungsinteressen beachten. Eine weitergehende Beantwortung der Frage wird ebenfalls in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.*

Bei der Funktion des Nachladens (hier „Online-Aktualisierung“ genannt) handelt es sich um eine Updatefunktion, damit z. B. bei einem Versionssprung der Kommunikationssoftware die Überwachungssoftware auf den neuesten Stand gebracht werden kann. In diesem Fall wird eine vom Softwarehersteller angepasste Software nachgeladen. Daher ist diese Funktionalität notwendiger Bestandteil der Beauftragung gewesen.

15. Trifft es zu, dass es sich bei der vom Anti-Viren-Software-Hersteller, Kaspersky analysierten Software, um den „großen Bruder“ des vom CCC untersuchten Staatstrojaners handelt, und wenn ja, welche Sicherheitsbehörden des Bundes und der Länder verfügen über diese Software?

---

* Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Weder zu der vom CCC, noch zu der durch die IT-Sicherheitsfirma Kaspersky analysierten Software liegen der Bundesregierung über die öffentlich verfügbaren Informationen hinaus Erkenntnisse vor. Eine Aussage, in welcher Beziehung die Programme zueinander stehen, ist daher nicht möglich.

16. Haben beauftragende Bundesbehörden vor Einsatz von Schadsoftware zum Infiltrieren von Computersystemen vor ihrem Einsatz im Einzelfall den Quellcode geprüft?

    Wenn ja, wie (intern/extern), existieren entsprechende Prüfberichte, wem lagen/liegen diese vor, und welches Ergebnis hatten sie?

17. Wurde hinterher geprüft, dass das eingesetzte Programm tatsächlich aus diesem Source compiled wurde?

    Wenn nein, warum nicht?

Auf die Antwort zu Frage 9 wird verwiesen.

18. Wie wurde jeweils sichergestellt, und wer hat die Einhaltung wie kontrolliert, dass die mit der Programmierung der Software beauftragten Firmen entsprechend zertifiziert sind, solche Aufträge durchzuführen?

Eine Zertifizierung für solche Aufträge ist gesetzlich nicht vorgeschrieben. Die seitens der Bundesbehörden beauftragte Fa. DigiTask befindet sich seit 2001 in der Geheimschutzbetreuung des Bundesministeriums für Wirtschaft und Technologie. Im Rahmen dieser Betreuung werden Mitarbeiter und Strukturen der Firma im Hinblick auf den Umgang mit amtlich geheimzuhaltenden Informationen (Verschlusssachen) überprüft.

19. Sahen und sehen die Lasten- und Pflichtenhefte der jeweils beauftragten Firmen vor, ein Sicherheitsaudit der Software durchzuführen, und wenn ja, wurde dieses Audit von einem unabhängigen Unternehmen oder einer anderen Institution durchgeführt, und wenn ja, von wem?

    Wenn nein, warum nicht?

Auf die Antwort zu Frage 7 wird verwiesen.

20. Haben die beteiligten Behörden hinreichend qualifizierte Mitarbeiter für ein Source-Audit?

    Wenn ja, um wie viele Personen handelt es sich jeweils (bitte nach Anzahl der Personen und Sicherheitsbehörde auflisten)?

Auf die Antwort zu Frage 9 wird verwiesen.

21. Sind Bundesbehörden technisch in der Lage, auch hard- oder softwarebasierte Angriffe auf Mobilfunkgeräte auszuführen?

Einzelheiten zu den technischen Fähigkeiten der Bundesbehörden können in diesem Zusammenhang nicht öffentlich dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Behörden des Bundes ziehen könnten. Im Ergebnis würde dadurch die Funktionsfähigkeit unserer Sicherheitsbehörden und mithin die Sicherheit der Bundesrepublik Deutschland

beeinträchtigt. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

22. Wie ist die Aussage der Bundesregierung in der Antwort auf die Kleine Anfrage auf Bundestagsdrucksache 17/5677 zu Frage 18 nach „Ferndurchsuchungen“ zu verstehen, wonach das Bundeskriminalamt die „für einen solchen Eingriff erforderlichen und den rechtlichen Voraussetzungen genügenden Einsatzmittel (sog. Remote Forensic Software) entwickelt“ habe, und welche Anwendungen sind hiermit gemeint?

Die vom BKA entwickelte Remote Forensic Software (RFS) wurde für Zwecke des verdeckten Eingriffs in informationstechnische Systeme (sog. Onlinedurchsuchung) durch das BKA gemäß § 20k des Bundeskriminalamtgesetzes (BKAG) entwickelt.

23. In wie vielen Fällen wurde der Einsatz der Überwachungssoftware mit jeweils welchem Funktionsumfang richterlich angeordnet bzw. genehmigt?

Die Onlinedurchsuchung durch das BKA wurde in insgesamt sieben Fällen angeordnet. Der Funktionsumfang der Überwachungssoftware ist auf die Vorgaben in der richterlichen Anordnung beschränkt.

Eine darüber hinausgehende Beantwortung dieser Frage ist der Bundesregierung aus Geheimhaltungsgründen nicht möglich. Nach der Rechtsprechung des Bundesverfassungsgerichts kann die Auskunftspflicht der Bundesregierung dort enden, wo ein auch nur geringfügiges Risiko, das im Rahmen einer Berichterstattung auch unter der Geheimschutzordnung des Deutschen Bundestages die angefragten detaillierten Informationen öffentlich bekannt werden könnten, unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, S. 78 [139]). Hierbei ist die parlamentarische Kontrollbefugnis mit den betroffenen Belangen, die zur Versagung von Auskünften führen können, abzuwägen (vgl. BVerfGE 124, S. 161 [193]).

Da es sich in diesem Fall um Auskünfte grundsätzlicher Art zur Anwendung von Ermittlungstechnik in Gefahrenabwehrverfahren nach § 20k BKAG handelt, könnte die Preisgabe von Informationen zum jetzigen Zeitpunkt die Anwendbarkeit dieser Vorschriften, die notwendigerweise in hohem Maße von der Geheimhaltung der sie ermöglichenden Technik abhängt, beeinträchtigen. Die Veröffentlichung dieser internen Vorgänge würde die Offenlegung sensibler polizeilicher Vorgehensweisen und Taktiken in einem äußerst gefährdungsrelevanten Bereich bedeuten und dadurch das schützenswerte Interesse der Bundesrepublik Deutschland an einem wirksamen Schutz vor Terrorismus erheblich gefährden.

Eine weitergehende Auskunft könnte Maßnahmen der Gefahrenabwehr erschweren oder gar vereiteln, weshalb aus dem Prinzip der Rechtsstaatlichkeit folgt, dass vorliegend das betroffene Interesse der Allgemeinheit an einer effektiven Gefahrenabwehr Vorrang vor dem parlamentarischen Informationsinteresse hat. Trotz ihrer grundsätzlichen verfassungsrechtlichen Pflicht, Informationsansprüche des Deutschen Bundestages zu erfüllen, muss daher im Ergebnis

* Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

nach Abwägung der betroffenen Belange das Informationsinteresse des Parlaments hinter den berechtigten Geheimhaltungsinteressen zurücktreten.

24. Gab es jenseits der obligatorischen richterlichen Prüfung im Rahmen des sog. Richtervorbehalts eine Überprüfung der jeweils eingesetzten Überwachungssoftware, und wenn ja, wer führte diese durch (bitte einzeln aufschlüsseln nach jeweiliger Behörde, Anlass für den Einsatz, konkretem Straftatverdacht, Rechtsgrundlage der Maßnahme, Anzahl der betroffenen Personen, Zeitpunkt und Dauer der Überwachungsmaßnahme, konkrete Einsatzfunktion – Kommunikationsüberwachung, Ausspähung und/oder Kopieren privater Daten (Speicherzugriff), Nachladen von Programmen, Kontrolle über den Rechner, Raumüberwachung usw. – und beauftragter Firma)?

Auf die Antwort zu Frage 6 wird verwiesen.

25. In wie vielen Fällen wurde eine andere als die vom CCC analysierte Überwachungssoftware durch Sicherheitsbehörden des Bundes und der Länder bislang eingesetzt (bitte einzeln aufschlüsseln nach jeweiliger Behörde, Anlass für den Einsatz, konkretem Straftatverdacht, Rechtsgrundlage der Maßnahme, Anzahl der betroffenen Personen, Zeitpunkt und Dauer der Überwachungsmaßnahme, konkrete Einsatzfunktion – Kommunikationsüberwachung, Ausspähung und/oder Kopieren privater Daten (Speicherzugriff), Nachladen von Programmen, Kontrolle über den Rechner, Raumüberwachung usw. – und beauftragter Firma)?

Die Überwachung der verschlüsselten Telekommunikation dient im repressiven Bereich der Verfolgung von Straftaten und im präventiven Bereich ihrer Verhinderung sowie der Abwehr von Gefahren.

Überwachungsmaßnahmen werden im repressiven Bereich auf § 100a der Strafprozessordnung (StPO) und im präventiven Bereich auf § 20l BKAG sowie § 23a des Zollfahndungsdienstgesetzes (ZFdG) gestützt. Es ist jeweils eine richterliche Anordnung erforderlich. Damit sind in der Regel ausschließlich die überwachte Person und deren jeweiliger Kommunikationspartner betroffen.

Art der Maßnahme	Straftat	Rechtsgrundlage, auf die die Maßnahme gestützt wurde	Zeitraum	Anzahl der betroffenen Personen
Bundeskriminalamt				
Strafverfahren	§§ 129a, 202a, 261, 263a, 303a, 303b StGB	§§ 100a, 100b StPO	keine Ausleitung	1
Strafverfahren	§§ 129a, 129b StGB	§§ 100a, 100b StPO	keine Aufbringung	0
Strafverfahren	§ 29a Abs. 1 Nr. 2 BtMG	§§ 100a, 100b StPO	09.09.2009 – 14.01.2010	2
Strafverfahren	§ 29a Abs. 1 Nr. 2 BtMG	§§ 100a, 100b StPO	keine Aufbringung	0
Gefahrenabwehr	§ 4a Abs. 1 BKAG	§ 20l Abs. 2 BKAG	15.02.2010 – 05.03.2010	15
Strafverfahren	§ 89a StGB	§§ 100a, 100b StPO	keine Aufbringung	0

Art der Maßnahme	Straftat	Rechtsgrundlage, auf die die Maßnahme gestützt wurde	Zeitraum	Anzahl der betroffenen Personen
Bundeskriminalamt				
Strafverfahren	§ 89a StGB	§§ 100a, 100b StPO	25.09.2010 – 02.12.2010	2
Strafverfahren	§ 89a StGB	§§ 100a, 100b StPO	keine Aufbringung	0
Strafverfahren	§ 89a StGB	§§ 100a, 100b StPO	07.10.2010 – 16.12.2010	7
Gefahrenabwehr	§ 4a Abs. 1 BKAG	§ 20l Abs. 2 BKAG	03.12.2010 – 26.01.2011	1
Gefahrenabwehr	§ 4a Abs. 1 BKAG	§ 20l Abs. 2 BKAG	keine Aufbringung	0
Gefahrenabwehr	§ 4a Abs. 1 BKAG	§ 20l Abs. 2 BKAG	keine Aufbringung	0
Strafverfahren	§ 263 Abs. 1 und 3 StGB	§§ 100a, 100b StPO	13.01.2011 – 10.10.2011	5
Gefahrenabwehr	§ 4a Abs. 1 BKAG	§ 20l Abs. 2 BKAG	keine Ausleitung	2
Gefahrenabwehr	§ 4a Abs. 1 BKAG	§ 20l Abs. 2 BKAG	keine Aufbringung	0
Gefahrenabwehr	§ 4a Abs. 1 BKAG	§ 20l Abs. 2 BKAG	keine Aufbringung	0
Gefahrenabwehr	§ 4a Abs. 1 BKAG	§ 20l Abs. 2 BKAG	keine Aufbringung	0
Strafverfahren	§ 29a Abs. 1 Nr. 2 BtMG	§§ 100a, 100b StPO	keine Ausleitung	1

Zollfahndungsdienst				
Gefahrenabwehr	§ 34 AWG	§ 23a ZFdG	keine Ausleitung	wird nicht erhoben
Gefahrenabwehr	§ 34 AWG	§ 23a ZFdG	keine Aufbringung	wird nicht erhoben
Gefahrenabwehr	§ 34 AWG	§ 23a ZFdG	keine Ausleitung	wird nicht erhoben
Strafverfahren	§ 34 AWG	§ 100a StPO	keine Ausleitung	wird nicht erhoben
Strafverfahren	§ 373 AO, § 95 Abs. 1 Nr. 1 ArzneimittelG	§ 100a StPO	27.10.10 – 14.04.2011	wird nicht erhoben
Strafverfahren	§§ 370, 373 AO	§ 100a StPO	keine Ausleitung	wird nicht erhoben
Strafverfahren	§§ 29a/30 BtmG	§ 100a StPO	keine Ausleitung	wird nicht erhoben
Strafverfahren	§§ 29a/30 BtmG	§ 100a StPO	keine Ausleitung	wird nicht erhoben
Strafverfahren	§§ 370, 373 AO	§ 100a StPO	18.09.2007 – 02.10.2007	wird nicht erhoben
Strafverfahren	§§ 370, 373 AO	§ 100a StPO	keine Ausleitung	wird nicht erhoben
Strafverfahren	§§ 29a/30 BtmG	§ 100a StPO	keine Ausbringung	wird nicht erhoben

Art der Maßnahme	Straftat	Rechtsgrundlage, auf die die Maßnahme gestützt wurde	Zeitraum	Anzahl der betroffenen Personen
Zollfahndungsdienst				
Strafverfahren	§§ 29a/30 BtmG	§ 100a StPO	Ende April 2007 – 19.07. 2007	wird nicht erhoben
Strafverfahren	§§ 370, 373 AO	§ 100a StPO	02.07.2007 – 05.07.2007	wird nicht erhoben
Strafverfahren	§§ 370, 373 AO	§ 100a StPO	11.12.2007 – 25.01.2008 21.05.2009 – 08.06.2009	wird nicht erhoben
Strafverfahren	§§ 370, 373 AO	§ 100a StPO	30.05.2009 – 09.11.2009	wird nicht erhoben
Strafverfahren	§§ 29a/30 BtmG	§ 100a StPO	25.09.2010 – 22.10.2010	wird nicht erhoben

Eine Übersicht über die auf §§ 1, 3 G10 gestützten Überwachungsmaßnahmen des BfV unter Einsatz der Quellen-TKÜ wird bei der Geheimschutzstelle des Deutschen Bundestages hinterlegt und zur Begründung auf die Antwort zu Frage 14 verwiesen.*

In Bezug auf den BND wird ebenfalls auf die Ausführungen in der Antwort zu Frage 14 verwiesen.*

Der Bund verfügt nicht über Erkenntnisse, welche Software Behörden der Länder bei Quellen-TKÜ-Maßnahmen eingesetzt haben.

26. Gab es bei Ermittlungsverfahren, in denen eine sog. Quellen-TKÜ oder eine Onlinedurchsuchung durchgeführt wurde, Amtshilfe zwischen einzelnen Landeskriminalämtern und Bundesbehörden, und wenn ja, in welchen Fällen geschah dies, in welcher Art und Weise (bitte einzeln aufschlüsseln nach jeweiligen Behörden, Anlass für den Einsatz, konkretem Straftatverdacht, Rechtsgrundlage der Maßnahme, Anzahl der betroffenen Personen, Zeitpunkt und Dauer der Überwachungsmaßnahme, verwendeter Software, Art der Amtshilfe)?

Die Bundespolizei (BPOL) hat im Rahmen eines Ermittlungsverfahrens wegen gewerbs- und bandenmäßigen Einschleusens von Ausländern im Jahr 2008 über sechs Wochen eine Quellen-TKÜ-Maßnahme auf Grundlage einer richterlichen Anordnung des AG München vom 3. April 2008 durchgeführt. Die technische Umsetzung der Maßnahme wurde nicht von der Bundespolizei selbst, sondern in Amtshilfe durch das Bayerische Landeskriminalamt vorgenommen.

Das BKA hat in drei Fällen in Amtshilfe für die Länder Quellen-TKÜ-Maßnahmen durchgeführt:

Bundesland	Straftat	Rechtsgrundlage, auf die die Maßnahme gestützt wurde	Zeitraum	Betroffene Personen
Hessen	§ 261 StGB	§§ 100a,100b StPO	23.03.2010 – 15.06.2010	20
Hessen	§§ 244 Abs. 1 Nr. 2, 244a, 25 Abs. 2, 53 StGB	§§100a, 100b StPO	keine Aufbringung	0
Rheinland-Pfalz	§ 250 StGB	§§ 100a, 100b StPO	25.11.2010 – 17.12.2010	1

* Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Maßnahmen der Onlinedurchsuchung wurden nicht in Amtshilfe durch das BKA umgesetzt.

Im Zusammenhang mit der Durchführung einer Quellen-TKÜ hat der Zollfahndungsdienst in keinem Fall einem Landeskriminalamt oder einer anderen Bundesbehörde Amtshilfe geleistet.

27. Wird durch das BKA oder andere Bundes- und Landesbehörden bei Onlinedurchsuchungen die gleiche Basissoftware wie für TKÜ-Maßnahmen (sog. Quellen-TKÜ) benutzt?

    Wenn nein, wer hat die bei Onlinedurchsuchungen verwendete Software entwickelt, wer hat die Software in welchem Rahmen geprüft, und wie viel hat die Entwicklung gekostet?

Im BKA werden Maßnahmen der Quellen-TKÜ und Online-Durchsuchung mit unterschiedlichen Softwareprodukten durchgeführt. Für die Onlinedurchsuchung wurde eine Softwarelösung durch das BKA entwickelt. Die Sach- und Personalkosten für die Entwicklung beliefen sich auf insgesamt 682 581,84 Euro.

Der Bund verfügt nicht über Erkenntnisse, welche Software Behörden der Länder bei Onlinedurchsuchungen eingesetzt haben.

28. Von wem wurde bzw. wird die entsprechende Überwachungssoftware (Frage 27) installiert und ausgeführt, wie geschah bzw. geschieht dies, und sind dabei auch Hardwareeingriffe am Rechner der überwachten Person notwendig?

Die Onlinedurchsuchungs-Software des BKA wird durch Mitarbeiter des BKA installiert und betrieben. Eingriffe in die Hardware des Zielrechners sind dazu nicht erforderlich.

29. Waren zur mittelbaren oder unmittelbaren Infektion des Zielrechners mit Überwachungssoftware Absprachen mit Internetdienstleistern notwendig, und wenn ja, in welchen Fällen, mit welcher Software, und mit welchen Telekommunikationsdienstleistern erfolgten diese, und wie waren die jeweiligen Unternehmen in die Überwachungsmaßnahmen involviert?

Einzelheiten zu ermittlungstaktischen Verfahrensweisen der Bundesbehörden können in diesem Zusammenhang nicht öffentlich dargestellt werden, da aus ihrem Bekanntwerden sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Behörden des Bundes ziehen könnten. Im Ergebnis würde dadurch die Funktionsfähigkeit unserer Sicherheitsbehörden und mithin die Sicherheit der Bundesrepublik Deutschland beeinträchtigt. Gleichwohl wird die Bundesregierung nach gründlicher Abwägung dem Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen nachkommen.

Die Informationen werden als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

* Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

30. Auf welche Art und Weise wurde Schadsoftware im Einzelfall in betreffende Rechnern eingebracht (bitte jeweils nach etwaigem physischem Eindringen in den Rechner/Wohnung oder manipuliertem Download auflisten)?

Die konkrete Aufbringung der Überwachungssoftware ist abhängig von dem in Einzelfall vom Beschuldigten verwendeten System. Die Befugnisse zur Onlinedurchsuchung und Quellen-TKÜ umfassen keine Eingriffe in das Grundrecht der Unverletzlichkeit der Wohnung aus Artikel 13 des Grundgesetzes.

Im Übrigen wird auf die Antwort zu Frage 23 verwiesen.

31. Wie setzt sich der Trojaner jeweils im System des Zielrechners fest, und welche Dateien sind davon betroffen?

Auf die Antwort zu Frage 30 wird verwiesen.

32. Waren und/oder sind Hersteller von Sicherheitssoft- oder -hardware (z. B. Firewalls und Virenscanner) in die Überwachungsmaßnahmen mit eingebunden, und wenn ja, in welcher Form geschieht dies?

Auf die Antwort zu Frage 29 wird verwiesen.*

33. Über welchen Weg gelangen die Daten vom überwachten Rechner zu den jeweiligen Ermittlungsbehörden, und welche Firmen, Behörden und/oder dritte Personen und Institutionen haben hierbei Zugriff auf die benötigten Server?

Zur Verschleierung des Kommunikationskanals der Überwachungssoftware werden die ausgeleiteten Daten über Server im In- und/oder Ausland verschlüsselt weitergeleitet. Eine Speicherung der ausgeleiteten Daten auf diesen Servern erfolgt nicht. Es handelt sich lediglich um eine Weiterleitung eines verschlüsselten Datenstromes. Dritte Personen und Institutionen konnten daher nach hiesiger Kenntnis keinen Zugriff auf die Daten erlangen. Die Verschleierung des Kommunikationskanals erfolgt aus taktischen Gründen.

34. Hat die Bundesregierung Kenntnis darüber, ob Sicherheitsbehörden in den USA auf die ausgespähten Daten Zugriff gehabt haben, und wenn ja, in wie vielen Fällen geschah dies?

    Wenn nein, wie kann die Bundesregierung dies ausschließen?

Die Bundesregierung hat hierüber keine Kenntnis. Durch Einsatz der beidseitigen Verschlüsselung kann mit an Sicherheit grenzender Wahrscheinlichkeit davon ausgegangen werden, dass Sicherheitsbehörden in den USA keine Kenntnis vom Inhalt der Daten nehmen konnten.

35. Wie stellen die Sicherheitsbehörden oder die mit der Überwachung beauftragten Firmen sicher, dass eine Manipulation der Ermittlungen, etwa durch eine auf diesem Übertragungsweg stattfindende Manipulation der Daten durch Dritte, verhindert wird?

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Insbesondere durch die beidseitige verschlüsselte Übertragung ist eine Manipulation der Daten durch Dritte eine rein theoretische Möglichkeit, da der Dritte Kenntnis über die IP-Adresse des Proxyservers, Übertragungsprotokoll, Verschlüsselungsverfahren und eingesetzten Schlüssel haben müsste.

36. Wie wurde und wird sichergestellt, dass der Überwachte nach einer möglichen Entdeckung der Software diese oder deren gesammelte Ergebnisse vor der Übersendung an die während der Überwachungsmaßnahme benutzten Server nicht manipulieren oder entfernen kann?

Die überwachte Person müsste nach Entdeckung eine derjenigen des CCC vergleichbare Analyse der Überwachungssoftware durchführen. Hierfür sind neben vertieften Fachkenntnissen entsprechende technologische Hilfsmittel und zeitliche Ressourcen erforderlich, die im Rahmen einer Überwachungsmaßnahme der überwachten Person nicht zur Verfügung stehen sollten. Darüber hinaus erfolgt die Übersendung der Überwachungsergebnisse unmittelbar parallel zur Telekommunikation des Überwachten. Ein Zugriff auf gespeicherte Daten findet nicht statt.

37. Kann sich die von den Sicherheitsbehörden genutzte Software selbstständig innerhalb eines Computernetzwerkes verbreiten, um so Zweit- oder Drittgeräte des Überwachten zu infiltrieren?

Nein.

38. Wie stellen die Sicherheitsbehörden sicher, dass bei der von ihnen genutzten Überwachungssoftware keine Programme oder Dateien auf das System der überwachten Person übertragen und/oder ausgeführt werden kann?

Bei von Bundesbehörden eingesetzter Software besteht eine Updatefunktion, mit der Updates (das heißt Programme bzw. Programmteile) auf das System der überwachten Person übertragen werden können. Der Funktionsumfang der Updates ist durch entsprechende Beauftragung des Softwareherstellers unter Berücksichtigung der richterlichen Anordnung bzw. des Beschlusses der G10-Kommission sowie der Vorgaben des Bundesverfassungsgerichts festgelegt.

Die Übertragung der Updates und die übertragene Datei werden protokolliert.

39. In wie vielen Fällen haben Infektionen mit staatlicher Schadsoftware dabei zum Versagen des Betriebssystems angegriffener Rechner geführt, und wie sind Schadensersatzansprüche hierzu geregelt?

Aus der aktuellen Berichterstattung in der Presse ist bekannt, dass in einem Verfahren der Staatsanwaltschaft Frankfurt/Oder eine Festplatte mit dem Überspielen eines Trojaners beschädigt worden sein soll. Der Bundesregierung liegen derzeit keine darüber hinausgehenden Informationen, insbesondere zu eventuell Schadensersatzforderungen, vor.

Mögliche Schadensersatzansprüche würden sich nach den allgemeinen Regeln des Staatshaftungsrechts richten. Für Maßnahmen des BKA im Rahmen seiner Zuständigkeiten nach §§ 4 bis 6 BKAG richten sich mögliche Ansprüche nach § 35 BKAG i. V. m. §§ 51 bis 56 des Bundespolizeigesetzes (BPolG).

III. Fragen zum möglichen Missbrauch der Staatstrojaner und zum Schutz unbeteiligter Dritter

40. Wie viele Fälle sind der Bundesregierung bekannt, in denen mit der Überwachung betraute Beamte oder Angestellte der damit beauftragten Firmen missbräuchlich an persönliche Daten, die durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschützt sind, gelangt sind?

Der Bundesregierung sind keine derartigen Fälle bekannt.

41. Welche Maßnahmen wurden durch die Sicherheitsbehörden getroffen, die einen solchen Missbrauch unrechtmäßig erlangter Daten der überwachten Personen oder unbeteiligter Dritter verhindern sollen, und inwieweit kann die Bundesregierung ausschließen, dass derartige Daten den Hoheitsbereich der deutschen Strafverfolgung verlassen?

Auf die Antwort zu Frage 35 wird verwiesen. Hinsichtlich der Daten, die den Hoheitsbereich der deutschen Strafverfolgung verlassen, wird auf die Antwort zu Frage 33 verwiesen.

42. In welcher Form und wie lange werden die im Rahmen der Überwachungsmaßnahme ermittelten Daten sowie deren Auswertungsergebnisse gespeichert, stehen diese Daten auch anderen Sicherheitsbehörden zur Verfügung, und wie ist sichergestellt, dass keine Unbefugten Zugriff auf diese Daten bekommen?

Daten, die mittels einer auf § 100a StPO gestützten Maßnahme erhoben wurden, werden nach Maßgabe der Strafprozessordnung, insbesondere den §§ 100a ff., 101 StPO, gespeichert und gelöscht. Die Zulässigkeit der Übermittlung solcher Daten für verfahrensübergreifende Zwecke bestimmt sich nach den §§ 474 ff. StPO.

Im Bereich der Gefahrenabwehr ist für vom BKA nach § 20l BKAG erhobene Daten § 20v BKAG maßgeblich für die Verwendung und Löschung der Daten. Für präventive Maßnahmen des Zollkriminalamtes nach § 23a ZFdG finden sich die entsprechenden Regelungen in §§ 23c und 23d ZFdG. Für Daten, die mittels einer Maßnahme nach § 3 Absatz 1 und 2 G10 erhoben worden sind, wird auf § 4 G 10 hingewiesen.

43. Wie wurde und wird der Schutz Dritter, die zufällig mit der überwachten Zielperson in Kontakt stehen, gewährleistet, und inwieweit werden diese Personen über die Überwachungsmaßnahme in Kenntnis gesetzt?

Gemäß § 20k Absatz 4 BKAG darf die Online-Durchsuchung zu Zwecken der Gefahrenabwehr durch BKA auch durchgeführt werden, „wenn andere Personen unvermeidbar betroffen werden“. In diesem Fall gelten die Benachrichtigungspflichten gemäß § 20w Absatz 1 Nummer 6 i. V. m. Absatz 2 und 3 BKAG, wonach „die Zielperson sowie die mit betroffenen Personen“ (Dritte) bei Vorliegen der entsprechenden Voraussetzungen über die Maßnahme zu benachrichtigen sind.

Gleiches gilt für die Quellen-TKÜ zu Zwecken der Gefahrenabwehr durch BKA. Gemäß § 20l Absatz 1 Satz 2 BKAG darf auch diese Maßnahme durchgeführt werden, „wenn andere Personen unvermeidbar betroffen werden“. In diesem Fall gelten die Benachrichtigungspflichten gemäß § 20w Absatz 1 Nummer 7 i. V. m. Absatz 2 und 3 BKAG. Demnach sind die „Beteiligten der betrof-

fenen Telekommunikation“ bei Vorliegen der entsprechenden Voraussetzungen über die Maßnahme zu benachrichtigen. Bei präventiven Überwachungsmaßnahmen des Zollkriminalamtes finden die §§ 23a ff. ZFdG Anwendung.

Sinngemäße Regelungen, die sowohl dem Schutz Unbeteiligter als auch bestimmter Kommunikationsinhalte dienen, enthalten §§ 3 Absatz 2, 3a und 4 Absatz 1 G10.

Bei einer richterlich angeordneten Quellen-TKÜ im Rahmen der Strafverfolgung sind gemäß § 101 Absatz 4 Satz 1 Nummer 3 StPO „die Beteiligten der betroffenen Telekommunikation“ zu benachrichtigen.

Für den Bereich des BND wird auf die in der Antwort zu Frage 14 genannte Anlage hingewiesen.*

44. Auf welcher Rechtsgrundlage wird Betroffenen nach Abschluss der Ermittlungen die Analyse des gegen sie eingesetzten Trojaners zur Überprüfung eventueller Grundrechtsverletzungen verweigert?

Der Bundesregierung sind keine Fälle bekannt, in denen Betroffenen nach Abschluss der Ermittlungen im Rahmen einer Überprüfung eine Analyse der gegen sie eingesetzten Überwachungssoftware verweigert worden ist.

IV. Fragen zur Sicherheitsarchitektur

45. Welche informellen Treffen, Arbeitsgruppen oder sonstigen Abstimmungen hat es zum Einsatz von Schadprogrammen zum Eindringen in andere Rechnersysteme auf Ebene von Bund und Ländern gegeben, und welche Arbeitsaufträge sowie Ergebnisse lieferten diese?

Im Jahr 2008 wurde eine RFS-User-Group eingerichtet, welche sich regelmäßig zusammenfindet, um rechtliche und technische Fragestellungen im Zusammenhang mit dem Einsatz von Überwachungssoftware (Quellen-TKÜ/Onlinedurchsuchung) erörtert.

Die Netzwerkforensik-Tagung, die seit dem Jahr 2010 einmal jährlich durchgeführt und durch das BKA ausgerichtet wird, dient in erster Linie dem Wissenstransfer im Bereich netzwerkforensischer Untersuchungen. Derartige Untersuchungen werden auch zur Aufklärung von Zielsystemen für die Vorbereitung von Maßnahmen der Quellen-TKÜ vorgenommen.

Die Quellen-TKÜ wurde im Verfassungsschutzverbund unter dem Gesichtspunkt des Erfahrungsaustauschs thematisiert. Konkrete Beschlüsse im Sinne gemeinsamer Forschung, Beschaffung oder Maßnahmendurchführung sind in den Gremien nicht getroffen worden. Die Besprechungen dienten in erster Linie dazu, einen Wissenstransfer zu leisten.

46. Kann die Bundesregierung die Aussage des Geheimdienstkoordinators im Bundeskanzleramt bestätigen, dass die Länderbehörden multifunktionale Rohlinge erhalten und diese von den Ermittlern je nach Vorgabe der zu-

* Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

ständigen Gerichte in ihren Funktionen reduziert werden, und von welchen Länderbehörden ist hier die Rede?

Der Koordinator der Nachrichtendienste des Bundes hat abstrakt generell Auskunft gegeben.

47. Welche Struktur, einschließlich der personellen Ausstattung zur Bündelung der Telekommunikationsüberwachung des Bundes und der Länder besteht inzwischen beim Bundesverwaltungsamt (BVA), und welche Rolle spielt das BVA bei den aktuellen Vorgängen?

Alle Aufgaben aus der Bündelung der Telekommunikationsüberwachung sind mit Ausnahme des derzeit noch erforderlichen Betriebs der gemeinsamen Anlage von BKA und BPOL an das BfV, das BKA und die BPOL zurückverlagert worden. Für den Betrieb stehen beim BVA noch 15 Personen zur Verfügung. Nach Abschluss der Rückverlagerung besteht keine Zuständigkeit des BVA für Telekommunikationsüberwachung mehr.

Im Übrigen sind Maßnahmen der Quellen-TKÜ niemals von der ehemaligen Zentralstelle für Kommunikationsüberwachung im BVA durchgeführt worden.

48. Wenn die zur Debatte stehenden Quellen-TKÜ-Maßnahmen nicht in letzter Instanz beim BVA koordiniert und ausgewertet werden, welche Abteilung welcher Bundesbehörde ist dafür zuständig, oder welche Bund-Länder-Arbeitsgruppe wurde zwischen Behörden oder Regierungsstellen oder im Rahmen der Arbeitskreise der Innenministerkonferenz (IMK) eingerichtet?

Für die Durchführung der Quellen-TKÜ durch BKA, Zollfahndungsdienst, BPOL, BfV sowie den Militärischen Abschirmdienst sind dort spezielle Fachbereiche zuständig. Die Koordinierung und Auswertung einzelner Quellen-TKÜ-Maßnahmen ist nicht Gegenstand von Arbeitsgruppen oder Arbeitskreisen der IMK, sondern erfolgt eigenständig durch die hierzu befugte Behörde.

49. Haben das BKA oder andere Bundesbehörden auch eigene Softwarelösungen zum Einschleusen von Schadsoftware auf Zielrechner oder zur Überwachung der Telekommunikation erarbeitet, und wenn ja, welche Funktionalität haben diese, welche Kosten sind dabei entstanden, wie oft und wann wurde von der Software Gebrauch gemacht?

Auf die Antwort zu Frage 27 wird verwiesen, soweit das BKA betroffen ist.

Die anderen Bundesbehörden haben keine eigene Software zur Durchführung von Quellen-TKÜ programmiert.

V. Fragen zum Export und europaweiten Einsatz der Spähsoftware

50. Welche Praxis bzw. Überlegungen für das Ausspähen fremder Rechnersysteme existieren durch die EU-Polizeiagentur Europol, auch hinsichtlich einer Koordinierung von Maßnahmen oder technischer Beratung/Hilfe?

Aktivitäten oder Überlegungen Europols betreffend die Ausspähung fremder Rechnersysteme im Sinne der Frage sind der Bundesregierung nicht bekannt.

51. Welche Geschäftsbeziehungen hatten Bundesbehörden bislang mit dem schweizer Unternehmen ERA IT SOLUTIONS AG, und welche Vereinbarungen haben sich hieraus ergeben?

Im Jahr 2007 wurde im Zollfahndungsdienst auf Software des schweizerischen Unternehmens Era-IT Solutions zur Durchführung von Quellen-TKÜ zurückgegriffen. Das Unternehmen hat sich 2008 aus diesem Geschäftsfeld zurückgezogen.

52. Stimmt der Pressebericht der „Neuen Zürcher Zeitung“ vom 15. Oktober 2011, wonach die schweizerische Bundeskriminalpolizei ein Rechtshilfegesuch an deutsche Behörden stellte, um „Mail-Verkehr und die Telefongespräche“ einer Züricher Linksaktivistin abzuhören, und falls ja, welche ergänzenden Mitteilungen kann die Bundesregierung hierzu machen?

Der Bundesregierung liegen keine über die Presseverlautbarungen hinausgehenden Informationen vor.

53. Mit welchen anderen Ländern haben Bundesbehörden Vereinbarungen getroffen, um ausländische Rechner mit deutschen Trojanern zu infiltrieren, und wie wurde dieser Eingriff in die Hoheitsrechte einer anderen Regierung jeweils geregelt?

Der Bundesregierung sind keine derartigen Vereinbarungen mit anderen Staaten bekannt.

54. Welche informellen Arbeitsgruppen oder sonstigen Treffen haben hierzu auf internationaler oder EU-Ebene stattgefunden, um grenzüberschreitende Einsätze behördlicher Schadsoftware zu regeln oder zu vereinfachen, und welche Verabredungen wurden dort getroffen?

    Wie wird die Bundesregierung den Beschluss des Europäischen Parlaments vom 27. September 2011 umsetzen, wonach Exporte von polizeilicher und nachrichtendienstlicher Überwachungstechnologie in Zukunft strengeren Ausfuhrkriterien unterliegen sollen?

Auf die Antwort zu Frage 45 wird verwiesen.

Mit dem Standpunkt vom 27. September 2011 (EP-PE_TC1-COD(2008)0249) hat das Europäische Parlament Änderungen der bestehenden Dual-Use Verordnung (EG) Nr. 428/2009 angenommen. Diese Änderungen sehen die Schaffung neuer allgemeiner Ausfuhrgenehmigungen der Europäischen Union vor. Bei allgemeinen Genehmigungen handelt es sich um Verfahrenserleichterungen für die Ausfuhr bestimmter Dual-Use Güter für unkritische Zwecke, deren Ausfuhr nach der bestehenden Verordnung (EG) Nr. 428/2009 genehmigungspflichtig ist. Die Allgemeingenehmigungen machen ein zeitintensives Einzelgenehmigungsverfahren für die Ausfuhr der in diesen Genehmigungen genannten Güter entbehrlich und stellen somit die Wettbewerbsfähigkeit der europäischen Exportindustrie sicher.

Die Änderungen der Verordnung (EG) 428/2009 beruhen auf einem Vorschlag der Europäischen Kommission. Im weiteren Verlauf des Rechtssetzungsverfahrens wurde zwischen Rat und Europäischem Parlament ein Kompromiss erzielt. In Kürze wird der Rat auf Grundlage des vom Europäischen Parlament am 27. September 2011 angenommenen Kompromisses die Änderungsverordnung zur Verordnung (EG) Nr. 428/2009 verabschieden. Diese Verordnung tritt am dreißigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen

Union in Kraft und gilt nach dem Inkrafttreten unmittelbar in allen 27 Mitgliedstaaten der EU.

55. Für welche aus Deutschland gelieferten „Abfangtechniken und Vorrichtungen der digitalen Datenübertragung, mit denen Mobiltelefone und Textnachrichten überwacht und die Internet-Nutzung gezielt beobachtet werden können“ kommt der EU-Parlamentsbeschluss nach Ansicht der Bundesregierung infrage?

Die angefragten „Abfangtechniken und Vorrichtungen“ sind nicht in der vom Europäischen Parlament angenommenen Allgemeingenehmigung für die Ausfuhr von Telekommunikationsgütern (EU 005, Anhang II f der Verordnung 428/2009) genannt und somit nicht für dieses vereinfachte Verfahren zugelassen.

Im Übrigen wird auf die Antwort zur Frage 54 verwiesen.

56. Wie beurteilt die Bundesregierung die Aussage von EU-Parlamentariern (PCWorld, 27. September 2011), wonach vor allem kleine Technologieunternehmen bezüglich kritischer Exporte intransparent sind?

57. Ist der Bundesregierung bekannt, dass zahlreiche deutsche Unternehmen regelmäßig mit Spionagesoftware auf internationalen Verkaufsmessen für Überwachungstechnologie teilnehmen, darunter neben DigiTask auch die Firmen Elaman GmbH, trovicor GmbH, ATIS UHER SA, ipoque GmbH und Utimaco Safeware AG?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

58. Wie bewertet es die Bundesregierung, wenn die genannten Unternehmen ähnlich unkontrollierbare Anwendungen wie der vom CCC analysierte Trojaner hierzulande wegen gesetzlicher Hindernisse nicht einsetzen dürfen, jedoch Märkte adressieren, in denen auch die Bundesregierung Menschenrechtsverletzungen durch Polizeien kritisiert?

Der Bundesregierung liegen dazu keine Informationen vor.

59. Haben deutsche Behörden jemals mit den Firmen Elaman GmbH, trovicor GmbH, ATIS UHER SA, ipoque GmbH und Utimaco Safeware AG geschäftlich zusammengearbeitet, bzw. hat sich eine der beiden Seiten jemals um eine solche Zusammenarbeit beworben, und falls ja, wann, und in welchen Fällen geschah dies, und welche Verabredungen wurden konkret getroffen?

Durch eine detaillierte Kenntnis über die Zusammenarbeit oder evtl. bestehende Verabredungen der Bundesregierung in ihrer Gesamtheit oder ihrer Ressorts im Einzelnen mit IT-Dienstleistern würde die Möglichkeit eröffnet, Rückschlüsse auf die bestehende IT-Infrastruktur wichtiger Einrichtungen der Bundesrepublik Deutschland und damit mittelbar auf deren Arbeitsweise zu gewinnen. Dieses bedeutet vor dem Hintergrund einer signifikant gestiegenen Bedrohungslage im Bereich der IT-Sicherheit und zahlreicher Angriffe auf IT-Einrichtungen des Bundes in jüngster Vergangenheit eine reale Gefahr für den Betrieb wesentlicher Einrichtungen des Staates. Diese Gefahr kann nicht hingenommen werden.

Zum Schutz der Arbeitsfähigkeit und der Aufgabenerfüllung der Einrichtungen des Bundes und damit mittelbar zum Schutz der Sicherheit der Bundesrepublik Deutschland ist die Bundesregierung daher nach sorgfältiger Abwägung zu der

Auffassung gekommen, dass die detaillierte Auskunft über Geschäftsbeziehungen von Bundesbehörden mit IT-Dienstleistern in derartigem Umfang grundsätzlich geheimhaltungsbedürftig ist. Gleichwohl ist die Bundesregierung nach gründlicher Abwägung bereit, das Informationsrecht des Parlaments unter Wahrung berechtigter Geheimhaltungsinteressen auch in diesem Fall zu befriedigen. Deshalb hat die Bundesregierung die erbetenen Informationen als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

60. Welche Stelle beim Bundes- bzw. dem Zollkriminalamt ist für testweise Nutzung von Abhör-, Spionage- oder Ermittlungssoftware zuständig?

Testmaßnahmen, die einer Beschaffung bzw. Nutzung einer Überwachungssoftware vorausgehen, werden durch die zuständige Fachabteilung Kriminalistisches Institut (KI) im BKA bzw. das technische Fachreferat des Zollkriminalamts durchgeführt.

61. Welche Bundesbehörden nutzen Produkte von der Firma rola Security Solutions GmbH, und um welche Anwendungen handelt es sich konkret bzw. welche Leistungsmerkmale und Schnittstellen zu welchen Datenbanken haben diese?

62. Welche Software nutzen Bundesbehörden zur Auswertung großer Datenmengen aus der Telekommunikationsüberwachung, und wird hierfür auch die Anwendung „Koyote“ von der Firma INTS GmbH genutzt?

    Falls ja, an welche Datenbanken ist diese über Schnittstellen angebunden, und über welche sonstigen Leistungsmerkmale verfügt diese?

63. Welche Software nutzen Bundesbehörden – auch testweise – von der Firma IBM Deutschland Research & Development GmbH, in welchen Feldern werden diese eingesetzt, um welche Anwendungen handelt es sich konkret, und über welche Features verfügen diese?

64. Sind Bundesbehörden jemals geschäftliche Beziehungen – auch testweise – mit den Firmen SPSS inc., humanIT Software GmbH, Inxight, In-Q-Tel oder L-1 Identity Solutions inc. eingegangen, und wenn ja, mit welchem Inhalt?

Auf die Antwort zu Frage 59 wird verwiesen. Aus den dort genannten Gründen hat die Bundesregierung die erbetenen Informationen als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag zur Einsichtnahme übermittelt.*

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333